METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SECURE FIRMWARE UPDATES

Abstract of the Disclosure

Methods, systems and computer program products which provide secure updates of firmware (*i.e.* data stored in a programmable memory device of a processing system) are disclosed. Updates of a programmable memory of a device may be controlled by providing an update window of finite duration during which the programmable memory may be updated. Access to the programmable memory may be based on the state of an access latch. The access latch may be set to allow access after a hardware reset of the device. An update control program may be executed to control access to the programmable memory and the latch reset to prevent access upon completion of the update control program. Verification of the update may be provided through encryption techniques and rules incorporated in certificates for application of updates to provide for selectively updating devices. Also disclosed are methods of securely providing differing functionality to generic devices.